Number 1-97

security awareness bulletin

Inside

Profile of a Spy

Department of Defense Security Institute, Richmond, Virginia

security awareness bulletin

Approved for open publication — Unlimited reproduction authorized
March 1997

Director
Department of Defense Security Institute
R. Everett Gravelle

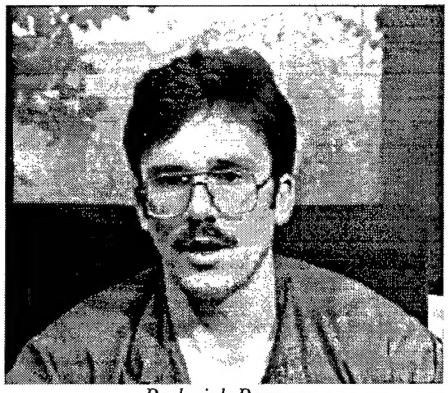
Editor
Lynn Fischer

The Security Awareness Bulletin is produced by the Department of Defense Security Institute, Richmond, Virginia. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and education methods.

For new distribution or address changes:

- Air Force: Contact your local Publication Distribution Office. Ask for "DODSISAB."
- Army, Navy, Marine Corps, and Department of Defense agencies: DoD Security Institute, Attn: SEAT, 8000 Jefferson Davis Hwy, Richmond, VA 23297-5091, POC Tracy Gulledge, (804) 279-4223, DSN 695-4223; fax (804) 279-6406, DSN 695-6406. E-Mail gulledget@dodsi.dscr.dla.mil
- DIS activities: HQ DIS/V0951, 1340 Braddock Place, Alexandria, VA 22314-1651.
- For other government agencies and contractors, you can order this publication through the Government Printing office (please see page 30), or download it from the Internet. Our URL is http://www.dtic.mil/dodsi

A Wasted Life:
The case of Roderick Ramsay



Roderick Ramsay

by Lynn Fischer
DoD Security Institute

Everything I had read about Roderick James Ramsay made me think, "Here's a gifted young man who for some unknown reason has deliberately thrown his life away as if on some trash heap." My three-hour interview with him at the Federal Penitentiary, Tallahassee, Florida, was to confirm that impression. I had gone to Tallahassee to interview Ramsay for the *Countering Espionage* series of security awareness videos produced by the Department of Defense Security Institute. Ramsay's quotes in this article are drawn from the tapes of this interview and are all included *in Profile of a Spy*. [See the product announcement that follows this article.] The interview itself offered no clear understanding of why he had allowed himself to become entangled in this self-destructive enterprise.

Entangled is not quite the right word – but it is clear he was selectively recruited by a slick and self-serving manipulator, Clyde Lee Conrad (at the time, U.S. Army Sergeant First Class) who apparently had little or no difficulty grooming the young service member as a source for classified documents that could then be sold to the Hungarian Intelligence Service. That was 1984, a year that marked the peak of the Soviet espionage offensive against the United States (with at least 11 new cases surfacing) and a time when the relentless Cold War showed no sign of abatement.

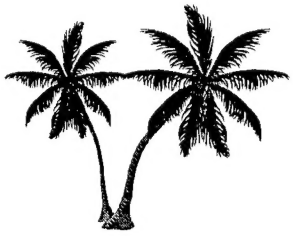
As the story opens, Ramsay was a U.S. Army sergeant in the U.S. Army Fifth Corps, operations specialist for the G3 Plans Section of the 8th Infantry Division, Bad Kreuznach, Germany. In his role of custodian for classified documents, he had accounting and safeguarding responsibility for all classified military and government documents maintained within the G3 Plans Section. He worked under Sergeant First Class Conrad's supervision for several months until Conrad's retirement the following year.

Conrad, later described as ringmaster of one of the most damaging espionage conspiracies ever to be inflicted upon the United States, was a product of recruitment himself. And, ironically, was recruited by another U.S. citizen in the early 1970s. The origins of this ring can in fact be traced to Hungarian-born ***Zoltan Szabo***, U.S. Army Captain and a veteran of the Vietnam War.

Szabo began working for Hungarian intelligence in 1967 and is likely to have been the product of "ethnic targeting" – recruitment attempts aimed at U.S. persons who, because of foreign birth or other cultural linkages might have conflicting national loyalties. Foreign intelligence spotters often consider a person in this category to be vulnerable to exploitation as a source of information.

When Conrad retired from the Army, having married a German national, he was allowed to remain in that country where he continued to draw upon several sources for classified materials who, like Ramsay, he had deftly recruited over the years. He apparently didn't know that Ramsay was following his example – selectively recruiting up to three others in his company for involvement in espionage. But this is getting ahead of the story.

Interview in Tallahassee



The Federal Penitentiary in Tallahassee is, despite the concertina wire, high fences, and heavily armed guards, something of a garden

spot among Federal facilities of its type. As we walked through the open courtyards to the interview room, it struck me that the tropical foliage and flowers seemed to clash with the cold steel of physical security. As mentioned earlier, Ramsay had agreed to have his interview taped for later use in one or more of our *Countering Espionage* awareness videos. He said that he was willing to talk to us to deter people like himself who might in the future be tempted to betray the trust placed in them. In this article, I am using his words to further that goal.

As I sat opposite the prisoner, I felt that whatever trust he had betrayed, however much he had deluded himself into thinking that he was committing no serious harm to his country, at least *now* he was being candid and open about the truth. He fully acknowledged his guilt and accepted the price to be paid for his crime. On the other hand, in retrospect, I am well aware that these offenders have had a lot of time to think about what they have done and how to explain it in a way that shifts as much of the culpability for the crime from themselves as possible.

Why espionage?

But why did it happen – it didn't make sense. The young man before us was neither naïve nor ignorant about the world; he seemed intelligent, level-headed, and articulate. He is said to be fluent in several languages – Japanese, Spanish and German – and to have the remarkable gift of near total recall of whatever he reads. He informed us that he was the product of a stable family environment where professionalism, "John Wayne-patriotism" and personal responsibility were high on the list of values.

But the nature of the crime and his betrayal of basic loyalty indicated that something was lacking in the makeup of his personality. Had some controlling mechanism been suppressed or destroyed, or had it been missing to begin with? There is no answer to this question, at least for the present. One day clinical psychologists may lead us to a fuller understanding of the mental workings of espionage offenders. All we can do here is to explore the known facts to better prepare ourselves for the future.

Sgt. Conrad ...managed to convince me that everything we were passing to the other side, they already knew anyway.

In the following case summary Ramsay's words, as recorded by our audio equipment, are shown in italics. I began the interview by asking him why this had happened:

Essentially it happened to me because I'm greedy...And the person that I trusted and worked for played upon my greed and convinced me to do a lot of things that I didn't think I would do."

Initial recruitment

Conrad had followed the pattern of many previously successful recruiters for espionage: First, fully ingratiating himself with the target, he then moved the target step by step into a pattern of cooperation and compromise by asking for innocuous favors and then full involvement. This incremental recruitment strategy is text book *modus operandi* used by agents developing sources of information. One of the best documented examples in the past was the case of William Bell who was skillfully manipulated by Polish agent Marian Zacharski in the late 1970s. Conrad used this slippery-slope approach against Ramsay.

Sgt. Conrad was my best friend in Germany, and he was also very much a mentor to me. He was sort of like a big brother or father figure.

It started with small things that he would ask me to do that weren't... they weren't illegal, but they weren't exactly ethical either. For instance, going out and photographing people he was meeting with, or carrying a sum of money from one country to another, which again, wasn't illegal, but if I had really actively looked at them, I'd have realized that it was the wrong road to be on.

Over a period of time, the small things that I did with Sgt. Conrad built up to the point where I knew that I

had compromised myself. And then Sgt. Conrad presented me with an opportunity or confronted me with a situation to commit an outright criminal act – go into our office and steal classified documents. And I chose to do so.

When he first asked me to copy classified material as my first overt illegal act, I was terrified. I was very, very scared. I was very, very nervous, and I was extremely worried that I was going to get caught. And when it was all over, I couldn't believe how easy it was.

Later, Conrad skillfully convinced Ramsay that what they were doing was really not damaging to the United States:

One of the conversations that Sgt. Conrad and I had on many different occasions centered around whether or not what we were doing was really harming the country. And he managed to convince me that everything we were passing to the other side, they already knew anyway. So that acted as sort of a sop to my conscience. I don't think there's any question that the idea that the Russians already had the knowledge contained in the material we were passing them made it easier for us to do what we were doing.

Ramsay was brilliant but erratic and enigmatic – a person who "in effect neutralized NATO."

But Ramsay was not fully convinced by this argument. He ultimately realized that what he was doing was wrong and injurious. And in retrospect, he realized that he had been manipulated by Conrad.

When you're actually doing this kind of thing you can't let your conscience talk to you or it will make you nuts. And my conscience started talking to me and started to make me nuts. And that's why I left the conspiracy. I don't think it ever bothered Sgt. Conrad. I don't think he had a conscience.

But was Ramsay all that pained by Conrad's amorality and plagued by a guilty conscience or was he, at the time, more concerned about being caught? Prosecuting attorneys, and FBI and U.S. Army agents paint a different picture of Ramsay's character.

Investigators described Ramsay as brilliant but erratic and enigmatic – a person who "in effect neutralized the North Atlantic Treaty Organization." Quoted in the *St. Petersburg Times*, FBI agent Joseph Navarro (who led the joint investigation) stated that Ramsay had a "powerful but criminal mind and had once confessed that he would even kill family members to further his espionage activities. His past brushes with the law included forgery and shoplifting and it is alleged that he had even plotted a successful armed bank robbery in Vermont in 1981. Navarro also recalled that he "didn't see any remorse over what he did – none whatsoever."

As I heard Ramsay's account for involvement in espionage from his own lips, it sounded too simple. It didn't ring true. I had a sense that something else was happening in this man's life that *he* didn't consider significant but *we* might: As was our normal routine in these interviews, I asked about job satisfaction, financial problems, subversive influences, romantic entanglements, psychological distress, substance abuse … and, there it was:

I didn't drink much during this time of my life, but I was smoking hashish quite a bit. I started smoking marijuana or hashish, whichever, when I was in high school probably when I was 15. But my usage while I was in the Army at the time in question was sometimes two to three times a week and sometimes not at all during the week. It just depended on the availability of the hashish and how I felt.

Ramsay held a Top Secret clearance. Had this question of drug use come up during his background investigation?

No, no one knew when I was getting my security clearance that I had any involvement with drugs, no one suspected...They asked me about drug use during the investigations. I lied.

In my later review of news reports of the case I came across a statement by the principal FBI investigative agent who said Ramsay claimed he had tried every drug under the sun.

Could drug use have clouded or impaired his judgment?

Despite long-term use of marijuana, hashish, and who knows what, Ramsay strongly discounted the role of narcotics in his personal decision to sell secrets to adversaries of the United States. He claimed also that he did not need money for drugs since he could afford the regular purchases with his salary.

I don't believe that the use of drugs affected my judgment, I think my judgment was poor to begin with. The people that I worked most closely with knew that I was taking drugs with the exception of Sgt. Conrad, but all of those people were taking drugs also. None of us considered it to be a problem. To be perfectly frank, I still don't.

Recruitment of others based on drug use

Whether it impaired his judgment or not, it is clear that drug use among Ramsay's coworkers played a dominant role in the enlargement of the espionage ring. In fact, it was the principal qualification for selecting co-workers for a recruitment pitch.

The people that I recruited, yes, they were involved in drugs, but it wasn't so much that they were pot smokers or hashish smokers that made them, in my opinion, more susceptible to the pitch. It was that these were people who had already shown a propensity or willingness to violate Army regulations.

Anyone in the Army who was willing to take drugs on a regular basis has to be willing to take some kind of risk and has to be willing to break the Army's regulations. That's the starting point.

Now, I know people who didn't smoke hashish in the Army but were only in for three years and smoked before they got in and intended to smoke when they got out, but they just weren't willing to break the Army rules. And so, those people I didn't think were approachable.

Ramsay, who claims to have recruited others in his section, was apparently accurate in his assessment of co-workers. In fact, two are currently in prison:

- *Jeffrey Stephen Rondeau*, arrested on October 1992 in Tampa, Florida, and charged with providing Army and NATO defense secrets, including tactical nuclear weapons plans to intelligence agents of Hungary and Czechoslovakia from 1985 until 1988. Rondeau was sentenced by a federal court to 18 years in prison in June 1994.

- *Jeffrey Eugene Gregory* arrested April 1993 at Fort Richardson, Alaska. According to an FBI official, Gregory who was active from March 1984 to October 1986, once packed a military flight bag with 20 pounds of classified documents for Conrad that included war plans for U.S. and NATO forces. In June 1994 Gregory was sentenced along with Rondeau to 18 years in prison.

So how does Ramsay feel about having recruited fellow service members for an illicit activity that led to their personal downfall? Had he no remorse about their fate? Did he have any sense of responsibility? His response was coldly indifferent:

To be honest, I really don't think about it. Everyone makes their own choices. I didn't choose for them. I offered them an opportunity and they leaped at it.
[Then he added] *I feel somewhat responsible,*

Regrettably, a determination in the clearance process that an individual is trustworthy does not immunize that person from a future betrayal of trust.

but there's nothing I can do about it so I don't deal with it.

Having brought Rondeau and Gregory into the operation, essentially as assistants to his covert activity, the flow of stolen documents to Conrad accelerated.

Modus operandi

The Conrad spy ring in which Ramsay played a key role was active in the mid-1980s. This was prior to the common use of computers in the workplace when the paper document was still the principal medium for classified information. Ramsay's methods were simple and depended largely on the photocopy machine, the help of his co-conspirators, and his own remarkable memory.

But his success in stealing information right under the noses of his supervisors was to some extent a function of the kind of blind faith we tend to have in co-workers who hold a security clearance. Regrettably, as we have seen in many espionage cases, a determination in the clearance process that an individual is to be considered trustworthy does not immunize that person from a future betrayal of trust.

Stealing the actual documents was extremely simple. I'd open the safe. I'd take the document out. I'd walk down the hall to the Sgt. Major's office. I'd flip up the lid of the copy machine. I'd burn off a copy of the document. I'd put the copy of the document in my briefcase, and then I'd go home. Or I'd read the document, and then when I got home, I'd take a little tape recorder and from memory read the document into the tape recorder.

At the end, I took out about 175 documents at one shot. Over the course of two weeks, I checked out all the NATO Secret documents...and I took all the Top Secret documents we had in the safe, and I took every Secret document I could get my hands on and spent two weeks at the photocopy machine just running them through the copier.

It was clear from what Ramsay said, that the loss of documentation over time was massive and at a very high level of classification.

My personal involvement in the conspiracy was from the spring of 1984 until January of 1986, but the conspiracy itself lasted from 1965 to 1988. I personally passed approximately 200 documents. The majority (of these) were classified Secret or NATO Secret. Approximately 10% were Top Secret. The total amount of money I received from Sgt. Conrad was in excess of $25,000 and at that time it seemed like a lot of money. But it wasn't worth it.

How to avoid suspicion

How could someone working in relatively close contact with about 35 people in an office unit and stealing large numbers of documents not have raised suspicions that would have been reported?

And a couple of times people asked me, you know, not in a suspicious manner, "Boy, you're really busy. What are you working on?" And I told them since I was getting fairly close to leaving, I had to take all these documents and review them and explain them to the Major who was in charge of the shops, since he'd never read them and it was his responsibility to know what they were. Of course, they believed that. So then I stored them in the mail bags we put our classified trash in before we took it down to have it burned.

The only time anyone would have possibly become suspicious about any of my activities is if they had seen me copying a Top Secret document. So what I would do is leave the Top Secret cover sheet in my office and not carry it with me to the copy machine. And they would have no idea of what I was copying.

I never copied anything on the weekend because that might be considered more suspicious than if I just copied it during the day time. We had a saying between Sgt. Conrad and me – "hide in plain sight." And that's just what we did. We didn't attempt to hide it.

When you attempt to hide, you make people suspicious.

Evading suspicion in the workplace was one thing, but what about after hours? Would people have noticed that he had a source of income significantly higher than military pay? Unexplained affluence has been a clear indicator in such recent cases as Aldrich Ames and Harold Nicholson.

The money went to partying which I guess you could say means going out on the town at night, spending $500 or $1000 on a single dinner party, visiting prostitutes, going to various casinos in Europe and spending money like it was water. Sgt. Conrad, on the other hand, invested most of his money in easily hideable items, specifically gold coins.

I never purchased an expensive automobile. One of the things that Sgt. Conrad and I talked about was not buying tangible items with the money that we were getting from our espionage activities because going out and buying something like a very expensive automobile was sort of like throwing up a red rocket and saying, "Hey, look what I have. Where did I get the money for this?"

The mother lode

According to evidence presented to the court at the time of Ramsay's trial, in late 1985 he had told co-conspirators Rondeau and Gregory that he was putting together a "mother lode" of documents for transshipment to Conrad. Gregory helped Ramsay stuff a military flight bag with 20 pounds of documents.

And the night I was ready to take them out, I stayed until about 5:30. I got an Air Force flight bag, took the two mail bags, dumped [the documents] into the flight bag, and toted them on out. That was all there was to it.

The volume of material demanded a more efficient method of recording the information and Ramsay discovered that videotaping the pages was much faster than photographing.

Court documents confirm that the stolen documents were passed through Conrad and then on to the Hungarian and Czech intelligence services. During this time, both services collaborated with the Soviet KGB. The information included:

- General plans for the allied defense of Central Europe
- Communications technology
- Coordination of NATO forces
- Information on the use of tactical nuclear weapons in NATO

The material that I personally stole and passed to Sgt. Conrad consisted of operational deployment plans and battle plans for the United States Army in Europe. However, the conspiracy had a much wider variety of information. I know that code was passed. I know that different decryption techniques were passed. That intelligence sources were passed. There was a great deal of material being passed.

Thirty pieces of silver

Despite Ramsay's professed greed, what did he actually gain from all of this activity? For the vast assortment of information that he contributed to Conrad's total haul, Ramsay's payoff ($20,000) was negligible compared to the potential value of the information. FBI Agent Allen H. McCreight commented at the time of Ramsay's sentencing in 1992, "It is incomprehensible that an American citizen could even think of doing this – all for a proverbial 30 pieces of silver – $20,000." This also stands in contrast to the earlier FBI estimate of the total netted by the ring during the course of its operation: between $2.5 and $5 million. The German court had in fact ordered Conrad, at the time of his conviction in June 1990, to surrender $1.7 million and all personal property.

One might ask, had these people no shred of loyalty to their nation that might have held them back from this criminal act? National loyalty is always an interesting issue to raise with espionage offenders. Ramsay's response was similar to others we have heard: He frankly admitted that he couldn't account for the profound contradiction between his history of betrayal and his supposed sense of national loyalty.

I think at the time I was almost sort of a dual person. In my actual Army life, I was extremely loyal to the United States and to the Army and would have been more than happy to pick up a rifle and walk to the front and do what needed to be done. And yet at the same time, I was stealing documents from the government, passing them to Sgt. Conrad, and he passed them on to the Hungarian intelligence service in exchange for money. And I've never been able to reconcile those two things.

Known by the sign of the cow bell

But he apparently had a stronger allegiance to the conspiracy. Having proven to Conrad that he was an effective source of highly classified materials, Ramsay was made aware that the espionage ring was active in more than just his unit. In early 1986, Conrad gave Ramsay a miniature cow bell on a key chain and told him any one who displayed a similar cow bell was involved in Conrad's activities.

At the beginning of my involvement , I knew almost nothing about the Conrad organization. By the time I left the conspiracy, I knew a great deal, an awful lot of details about the organization. I met several other people...including the Kercsik brothers who were couriers for us, other people that Sgt. Conrad said were stealing documents for him, and members of the Hungarian intelligence service.

I traveled for meetings with these people to Meinz, to Wiesbaden, to Salzburg,, Linz, and Innsbruck in Austria. Mostly southern Germany and Austria. I never traveled behind the Iron Curtain. There was no reason to.

Getting out, but not quite

According to Ramsay's account, by late 1985, he was getting very uncomfortable and wanted out of the covert activity. But he was afraid of Conrad and how he would react if he simply terminated the relationship.

In the summer of 1985, I intentionally failed a urinalysis test and used that to get out of the Army without being pressured by Sgt. Conrad to reenlist. I was discharged in November and went back to live in Boston.

But it wasn't over. Ramsay claims that Conrad had insisted that he agree to smuggling export-controlled computer chips to Conrad based on a shopping list provided by Hungarian intelligence. But eventually he told Conrad that he wanted out altogether.

I didn't actually send out any chips. I got the information needed to begin the operation, gave it to Sgt. Conrad and at that meeting told him I was through. He finally told me, "Okay, fine, I don't ever want to see you again. Just make sure you never say anything to anyone. If you do, you're dead."

The ring is rounded up

Clyde Lee Conrad was arrested on August 23, 1988. Lt. Gen. (Ret.) William Odom was quoted in the press as stating that in the early 1980s counterintelligence knew there was a problem, but Conrad was not identified as the perpetrator until much later. In 1989 he was charged with treason under West German law. He was convicted and sentenced to life imprisonment in June 1990 following a U.S. Army investigation. He is now serving his time in a German penitentiary.

Arrested at the same time as Conrad were Imre Kercsik and Sandor Kercsik (brothers), both medical doctors of Hungarian origin residing in Sweden who acted as couriers for the spy ring throughout Western Europe. The Kercsik brothers were convicted by a Swedish court in late 1988 for espionage but were given a light sentence of only 18 months in prison since the act did not target Swedish interests.

In sentencing Conrad, the German judge stated that Conrad's motives for spying were "pure greed," he

had "endangered the entire defense capability of the West," and that had war broken out, the information passed by Conrad "could have led to a breakdown in the defenses of the Western Alliance" and to "capitulation and the use of nuclear weapons on German territory."

According to Sandor Kercsik who spoke freely about the conspiracy, it all began for him in 1967 when he first met Szabo in Vienna. Szabo himself was convicted of espionage by an Austrian court in 1989, but received a 10-month suspended sentence because of his cooperation with authorities in the prosecution of Conrad.

Ramsay was arrested on June 7, 1990 (the day after Conrad's conviction) in Tampa where he had lived for two years, engaged in occasional labor as a busboy and cab driver. He had been nearly destitute and living in a small house trailer owned by his mother, frequently sleeping in his car. Ramsay had anticipated his own arrest since Conrad's apprehension in Germany. Ramsay admitted his collaboration with the spy ring and was held without bond to await trial.

On September 18, 1991, under a plea bargain Ramsay pled guilty to one count of espionage and agreed to assist in the further investigation of the conspiracy. He was sentenced in August 1992 to 36 years in federal prison. The prosecuting U.S. attorney stated that the lenient sentence reflected Ramsay's cooperation with the on-going investigation. The arrests of Jeffrey Stephen Rondeau and Jeffrey Eugene Gregory followed within a few months.

According to Special Agent Navarro, during the investigation before the arrest, FBI and U.S. Army agents learned that Ramsay had stashed Top Secret documents at his mother's house in Tampa and later destroyed them after the arrest of Conrad in 1988. In June 1990 agents searched the home but found nothing.

The Italian connection

There is one other member of the spy ring who has been identified in open sources or the public media: Thomas Mortati, a U.S. Army paratrooper, who was arrested in 1989 in Vincenza by Italian authorities on charges of having passed Top Secret documents also to Hungarian military intelligence services. Italian-born Mortati is said to have disclosed classified information about American and NATO bases in Italy. Mortati, a naturalized U.S. citizen left the Army in 1987 but remained in Italy as his American wife continued to work for the U.S. Army base in Vincenza. According to media reports, Mortati was recruited in 1981 by Szabo.

He is said to have confessed to Italian authorities that he attempted to bribe several Italian officers in 1984 and 1985, offering money for information. He also claimed to have been paid $500 a month by the Hungarian intelligence service. Mortati was convicted in an Italian court and after a period of incarceration has been released.

Summary and lessons learned

According to the FBI Tampa field office chief, "Not only was this the most extensive espionage investigation in the history of the FBI, but it was considered to be the largest U.S. espionage conspiracy case in modern history." Eight men were arrested and convicted by U.S. or European courts. Four of the eight are currently serving prison terms for their crimes. The focus of this story has been on only one of the offenders – but the one among them who engineered the more extensive thefts of classified materials from their place of safeguarding.

Regardless of what Ramsay told us in his interview, we should not rush to judgment about the security climate of the U.S. Army Europe in the late 1980s or conclude from his statements that use of drugs by service members was out of control. We would have to look for other, more objective, assessments of the situation in order to determine that the organizational environment was in fact a major contributing factor in this crime of betrayal. Incarcerated offenders have the time and a reputation for concocting new versions of history to help justify the apparent mindlessness of their past behavior.

Furthermore, from the point of view of the security educator, we run a risk in zeroing in on people like Ramsay or Conrad who are deviants in the vast population of loyal and trustworthy military service personnel and civilian employees: We might lose

sight of the fact that our national survival through the Cold War era and even unto the present day has rested on the prevailing integrity of those who have been entrusted with privileged information and who have neither lost nor sold it for personal gain. While we examine the more sensational aspects of espionage, we should also be saluting the people who have lived up to their security responsibilities, for a job well done. But we can do even more to prevent espionage in the future.

What we know from Ramsay's own account and from official sources about the Conrad spy ring lead us to several lessons learned which reinforce truths we have drawn from other episodes of this type:

- If anything regarding the handling, safeguarding, or processing of classified information or materials doesn't look right, a concerned employee should follow up on the issue (possibly with a confidential word with a security officer) until he or she feels that the question has been resolved and is comfortable with the explanation.

- In this age of security risk management, we are not going to implement every possible safeguard, physical check, or accounting procedure regarding classified materials. But we can make sure that those reasonable security measures are observed that conform with policy and which meet the needs of that time and place based on a threat assessment and the potential damage if a compromise takes place.

- A security clearance for any level granted at one point in time is no absolute guarantee that an employee in a position of trust won't betray that trust in the future. People change over time and their life situations change as well – sometimes for the worse. The principle of *continuing evaluation* is still valid.

  We owe something to the people with whom we work and share a responsibility for guarding the nation's secrets: What we have seen in many of these cases is a failure of co-workers and supervisors to intervene when they see a personal problem that needs to be addressed. It then becomes a security problem or worse. Whether it be reporting in confidence to a security professional or referral of an individual to an employee assistance program, something must be done when it appears that an employee appears not to be coping with a significant problem.

- Lastly, it has been shown repeatedly that those few people who get involved in and are subsequently arrested for espionage had the illusion they were so smart that they could avoid detection. Wrong! By counterintelligence methods, by confidential sources, or by defections from adversarial intelligence services, eventually they will be identified and end up paying big time. It's inevitable.

I was thinking as I passed through the prison's sally port: If Roderick Ramsay serves his full sentence of 36 years, he will be 66 years old when he is released if he lives that long. Could Ramsay, and Gregory and Rondeau as well, have been spared this fate if an alert and conscientious co-worker had seen a warning sign and intervened in some way? I don't know if Ramsay has a "criminal mind" or was so muddled by drugs at an early age that his judgment will always be skewed. But, given the talents that this person had to offer, what a waste!

My involvement in espionage activity wrecked what was, for me, a promising military career. It was part of the reason I didn't pursue my dreams of going to college. And when everything came to pass as far as legal ramifications, I ended up with a 36-year sentence in the federal prison system, and it's, I guess you could say, fairly horrible. You're fenced in like a wild animal. The people that you deal with have absolutely no respect for you anymore. And you're basically treated like an animal. And I certainly didn't envision having anything like this happen to me when I got involved.

Announcing the Release of a new Video
by the Department of Defense Security Institute

Profile of a Spy

A 90-minute video document of an interview with convicted espionage felon Roderick Ramsay, recorded at the Federal Penitentiary, Tallahassee Florida

This video has been produced to support training programs for counterintelligence and security professionals. It may also be used by security educators in support of security awareness programs for cleared personnel. For security awareness, however, we recommend showing selected segments to meet particular educational objectives. A *Presenter's Guide* and a printout of the full interview transcript (with timings) is provided with each copy of the video.

Copies may be obtained through FilmComm Inc., 641 North Avenue, Glendale Heights, Il 60139. Call in advance for current pricing. (603) 790-3300.

Because of sensitive information included in the interview, this product is marked and distributed as For Official Use Only (FOUO). For this reason we must ask contractor facilities to order by letter stating that the material will be used only in support of government security programs, and will not be released to the public media.

Challenge Inspections under the Chemical Weapons Convention (CWC)

The United States is one of 156 signatories to the Chemical Weapons Convention (CWC) which will come into force on 29 April 1997. It will prohibit the development, production, stockpiling and use of chemical weapons. One of several verification provisions of the CWC is the use of "challenge inspections" at any government, private or commercial facility to demonstrate that prohibited activities are not taking place. A team of multinational inspectors who are employed by the CWC's implementing body, the Organization for the Prohibition of Chemical Weapons (OPCW), will conduct the inspections.

While any signatory nation may request an inspection of any other signatory nation's facility, the facilities most susceptible to challenge inspections will be those that manufacture or use large volumes of chemicals and chemical products. The suspicion of production or stockpiling of Chemical Weapon (CW) agents or precursor chemicals may serve to justify a challenge inspection. Prohibited and controlled chemicals are listed in the CWC.

The CWC outlines detailed time lines for challenge inspections at both declared and undeclared facilities. For example, the Director-General of the OPCW must notify the U.S. of a challenge inspection no less than 12 hours before the inspection team may arrive at the point of entry (POE). For a site that has not been declared to be a U.S. chemical weapons-related facility, the inspection team will arrive at the facility no later than 36 hours following arrival at the POE. Once the inspection begins, it may last no longer than 84 hours, unless the U.S. government agrees to an extension.

During a challenge inspection, the inspection team has the right to monitor all traffic exiting the facility; take air, soil or effluent samples; request to have photographs taken; review records and interview employees. They may also request an overflight of the facility. However, inspectors are obligated to conduct their inspection in the least intrusive manner possible. The U.S. will apply a managed access provision of the CWC to all inspections activities.

Should a challenge inspection occur at a commercial facility, U.S. representatives will request the assistance of facility managers in negotiating the amount and type of access an OPCW inspection team will need to confirm compliance with the CWC. The amount of access may be limited in order to reduce inspector access to activities unrelated to the CWC.

Proper planning can reduce the risk to national security and proprietary information. Planning should take full advantage of CWC protective rights including the removal of sensitive papers, shrouding sensitive equipment or control panels, and managing inspector access within your facility. Planning should also consider alternative means to satisfy compliance concerns.

For more information on CWC Challenge Inspections, please contact the On-Site Inspection Agency Defense Treaty Inspection Readiness Outreach Program at 1-800-419-2899.

The CWC— Reporting Obligations for Defense Industry

Mike asked Larry how his trip was to the Defense Treaty Inspection Readiness Program (DTIRP) annual seminar in Washington, DC. Larry answered, "I received a lot of information about different arms control agreements which could affect us. As the Facility Security Officer, I need to be up to speed on these things." Mike asked, "Was there anything in particular you heard that I need to be concerned about?" Larry replied, "I'm glad you asked because I want to ask you some questions about our use of certain types of chemicals."

The Chemical Weapons Convention (CWC) bans the research, development, production, stockpiling, transfer and use of chemical weapons and includes reporting requirements which directly affect U.S. defense industry. Chemical-producing, processing or consuming defense contractors should be aware of CWC reporting requirements and their potential impact with regard to protecting confidential business and proprietary information.

What is the Chemical Weapons Convention?

More general security information about the CWC is available. Contact OSIA's Industry Outreach Program Manager at 1-800-419-2899 for a variety of free, useful materials such as: the "Questions Facing U.S. Defense Industry" pamphlet; a comprehensive CWC briefing; or a video entitled "The CWC and Its Impact on U.S. Facilities."

Currently, 160 nations have signed the CWC. Entry into force (EIF) will occur six months after 65 of those nations ratify the Convention. The CWC requires that all parties to it routinely report certain types of information concerning production, use, transport, export and import of scheduled chemicals. The purpose of reporting is to allow monitoring of the production and utilization of chemicals which can be easily manipulated for chemical warfare purposes.

These chemicals are grouped into three "schedules" based on their previous use or potential use in chemical weapons. Schedule 1 chemicals comprise actual chemical weapons agents and chemicals that have a high potential for use in activities prohibited under the CWC. As defined under the CWC, they have, for the most part, little or no use. Schedule 2 chemicals include several toxic chemicals and many precursor chemicals. Chemicals listed in Schedule 3 are also known as "dual-use" chemicals because, while they are also precursor chemicals, they are produced in large quantities for many legitimate commercial purposes, such as for use in dyes, inks, pesticides and pharmaceuticals.

The CWC also monitors the production of certain levels of other unscheduled chemicals called "discrete organic chemicals," as well as discrete organic chemicals containing phosphorus, sulfur or fluorine (PSF).

Larry, I don't understand," said Mike. "Just because we produce a chemical or two listed under Schedule 3, we have to submit detailed reports on our processes to the government? There are lots of good uses for the chemicals we produce. I can't believe that every company that uses these has to supply reports." "No Mike, every company doesn't have to. It depends on several factors," said Larry. "Look at this chart – it shows the criteria and threshold amounts that trigger a reporting requirement."

Declaration (reporting) requirements are determined by chemical types and quantities. The check marks in the following chart depict reporting obligations. Note that the difference between declaration and inspection thresholds is based upon the quantity of the chemical involved.

Criteria	Chemicals				
Schedule	1	2	3	DOC	DOC PSF
Previous Year(s)	1	3	1	1	1
Projected Year	1	1	1	1	1
Production	✓	✓	✓	✓	✓
Consumption	✓	✓			
Process		✓			
Storage	✓				
Transfers	✓	✓			
Import		✓	✓		
Export		✓	✓		
Reporting Threshold	10kg	1kg* 100kg** 1 t***	30 t	200 t	30 t
Inspection Threshold	10kg	10kg 1 t 10 t	200 t	200 t	200 t

DOC = Discrete Organic Chemicals
PSF = Phosphorus, sulfur, fluorine
kg = kilogram
t = tonne (metric measurement)
* Schedule 2, Part A designated with an *
** Schedule 2, Part A
*** Schedule 2, Part B

For a complete list of chemicals monitored by the CWC, contact the Public Information Office of the Arms Control and Disarmament Agency (ACDA) at (202) 647-8677.

Schedule 1

✓ *Any* scheduled chemical activities your company was involved in that were directly related to chemical weapons production or research must be included in initial reports. This includes provision of data on chemical weapons related equipment at any time since *1946*.

✓ If during the year prior to CWC EIF you have produced 100 grams or more of a Schedule 1 chemical for research, medical or pharmaceutical purposes, you are subject to CWC reporting requirements.

Schedule 2

✓ Likewise, you would be required to provide CWC data declarations if, during any of the three previous calendar years, you produced, used, or processed more than 1 kilogram of the hallucinogen BZ, 100 kilograms of the toxic chemicals Amiton or PFIB, or 1 metric ton of any other Schedule 2 chemical. Also, if your company plans to produce, use or consume those same quantities or more of Schedule 2 chemicals in the coming calendar year, you would also have to report that information.

Schedule 3

✓ If you have produced in the previous year, or plan to produce in the coming year, more than 30 metric tons of any Schedule 3 chemical, you must report that, too.

Discrete Organic Chemicals

✓ If, during the last year, your company produced more than 200 metric tons of discrete organic chemicals or more than 30 metric tons of a discrete organic chemical containing a PSF chemical, you must submit CWC data declarations.

✖ Facilities that produce pure hydrocarbons or explosives are exempt from CWC reporting requirements.

Well Larry, I understand the concern over Schedule 1 chemicals, but there must be thousands of companies like us that produce Schedule 3 and discrete organic chemicals. What happens when all of us declare our chemical activities at the same time?" "I'm glad you said 'declare' Mike," replied Larry, "because that's just what the Office of National Authority will do. We, and all those other facilities that meet any threshold for reporting, will be deemed 'declared sites' and reported as such to the OPCW."

The Organization for the Prohibition of Chemical Weapons (OPCW) is an international body charged with overseeing CWC implementation. It will determine report formats and will be the recipient and retainer of all declarations.

Preparation of CWC declarations will begin with the facility or its parent company providing the report to its Department of Defense (DoD) or Department of Commerce (DOC) sponsor. Next, the DoD or DOC sponsor will forward these declarations to the Office of the National Authority (ONA), co-located at the Arms Control and Disarmament Agency in Washington, DC. The ONA will collate all U.S. declarations into an aggregate declaration and submit it, along with declarations from plant sites, to the OPCW at The Hague, Netherlands.

Facilities that are included in the U.S. aggregate declaration will be designated "declared" sites. Those sites meeting the inspection threshold quantity, as shown in the chart, will be subject to initial and/or systematic routine inspections by international inspection teams from the OPCW.

These reports sound more important all the time Larry," Mike said in a more concerned voice. "We definitely exceed the reporting threshold for Schedule 3 reporting requirements according to this chart. What goes in the report and when is it required?"

As a CWC signatory, the U.S. must submit its first data declaration within 30 days after the Treaty takes effect. For most chemicals, the initial and subsequent annual declarations require only historical data about certain chemical uses for the previous three years and projections for the coming year.

Initial Declaration

For each Schedule 3 chemical, sites must provide the chemical name, formula, and aggregate quantity produced, as well as amounts of Schedule 3 chemicals imported and exported by country. In addition to the historical data, initial declarations for Schedule 3 sites will include the name and precise location of the site.

Annual Reports

After the initial declarations for Schedule 1 and 2 chemicals, facilities will have to file two annual reports updating their declarations: (1) a report giving estimates of anticipated production and use of CWC-monitored chemicals for the coming year, due 60 days prior to the beginning of the year; and (2) a report on the past year's production and use, due 90 days after the end of the year. Any additional activity that is planned after the initial declaration is submitted must be reported five (5) days prior to the start of that activity.

For Schedule 3 chemicals, only data on amounts of chemicals produced, as opposed to how much used, must be declared for Schedule 3 sites. Because the OPCW will be looking for large-scale production of these chemicals, on-hand inventory quantities will be supplied in ranges of tonnage. For facilities that export or import chemicals, information about the recipient or supplier must also be provided.

Changes in Activities

Another report required by the CWC applies to facilities that anticipate significant changes in scheduled chemical activities after their initial or annual data declarations are filed. These sites must file another report to update the declaration at least five days prior to the start of the activity.

Mike's eyes were wide open now and it was obvious that he understood the potential economic impact this information could have if it were used inappropriately. He asked Larry, "What assurances do we have that our reports will not be openly divulged?" "You have a valid concern, Mike," said Larry, "but the CWC takes care of it."

Initial CWC declarations and all annual reports retained by the OPCW will be treated with confidentiality. This includes secure storage, limited distribution on a need-to-know basis, and sanctions for breaches of confidentiality. Moreover, OPCW personnel must sign confidentiality agreements to not divulge the information during and after their employment.

Nevertheless, concerned facilities may want to begin the process of determining their potential security concerns with regard to CWC reporting. Learning more about the CWC and its reporting obligations can help you assess any risk to proprietary and other sensitive information at your facility.

If you think your facility or company may meet a CWC reporting threshold requirement, but you are not sure if you should be a declared site, notify your sponsoring agency, local DIS Industrial Security Representative, or contact OSIA's Outreach Program Manager at 1-800-419-2899. Assistance and guidance is available to help you prepare for CWC reporting requirements while protecting proprietary and sensitive information.

"Mike, you still look a little concerned, what's on your mind?" asked Larry. "You said we should be a declared site, right? You also said declared sites may meet inspection thresholds. What inspections? What about international inspection teams? When?" Larry grinned, "Mike, you're putting this together pretty well now. Let's save that discussion for after lunch."

Facility Overflights under the Open Skies Treaty

The Open Skies Treaty allows foreign aircraft equipped with specified sensors to fly observation missions over the United States. These observation aircraft will be capable of imaging any facility in the continental U.S. or on the territory of another treaty signatory. The Open Skies Treaty may enter into force as early as mid-1997. Observation flights can begin within 90 days after entry-into-force.

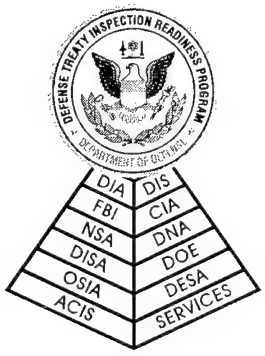
The United States and 26 NATO and former Warsaw Pact nations signed the Open Skies Treaty. Any signatory may conduct observation flights or "review data from flights" of any other signatory nation after the Treaty enters into force.

When the Treaty first enters into effect, observation aircraft will be allowed to carry panoramic, framing and video cameras as well sideways-looking synthetic aperture radar (SAR). During the first three years, observation aircraft will be allowed to carry infra-red (IR) scanning devices if both parties agree on that particular flight, but after three years, IR scanning may be used on any flight.

Even though sensor resolution is somewhat constrained, the sensors will provide information that cannot be acquired by commercial satellites. Industrial equipment, vehicles and minor facility modifications can be identified, and people engaged in activities can be detected.

The SAR permits observation aircraft to perform their missions in bad weather and at night. The infra-red scanner will allow the aircraft to "see" differences in the temperature of objects on the ground, especially operating machinery or vehicles, even through thin coverings such as camouflage netting.

Open Skies overflights may pose new risks for U.S. facilities that should be carefully assessed. Outdoor activities such as research, development, testing, evaluation, and modification programs on aircraft, helicopters, ships, tanks and other vehicles that are classified or sensitive may now be at risk. Signatures or indicators – such as plant layouts, power sources, ventilation systems, cooling ponds, and pollution of vegetation – that could reveal proprietary information to a highly skilled analyst should also be assessed. In many cases, a potential problem can be solved by properly covering or moving an item of concern inside prior to an Open Skies overflight mission.



The Department of Defense has established the Defense Treaty Inspection Readiness Program to assist the U.S. government and contractor community in limiting the loss of information during inspections or overflights of U.S. facilities under arms control agreements. DTIRP has developed an early warning notification system, that is derived from the agreed Open Skies flight plan, to notify facilities that could be imaged during an overflight.

This automated notification system can provide various types of advance warning beginning with the initial 72 hour notice of intent to conduct an observation flight in the U.S., through notification of imminent flight departure for the mission. Upon request, your facility or facilities can be included in the notification system.

DTIRP can provide you with more information on Open Skies overflights and notifications. Please contact the On-Site Inspection Agency Defense Treaty Inspection Readiness Outreach Program Manager at 1-800-419-2899.

Open Skies Overflights – What Will They See?

Mike said to himself, "Well here's something I've never seen before," as he opened the Open Skies Treaty Data Call package that had arrived with the morning mail. It contained a computer disk and information from the Pentagon and the On-Site Inspection Agency. Mike had recently taken over as site manager for Defense Tech, Inc., so his first reaction was to forward the package to Larry, his facility security officer and newly designated point of contact for information about arms control treaties. But, as he placed the contents back into the envelope, part of the Pentagon's memo caught his eye: "It allows for unarmed aerial observation flights, unrestricted...with a variety of still photography, infrared and video cameras and an all-weather radar system to record the ground...." He decided to call Larry instead, "I just received a big package from the Defense Department, come and tell me what you know about observation flights carrying cameras."

Early in 1994, at the direction of the Office of the Under Secretary of Defense for Acquisition and Technology, the On-Site Inspection Agency mailed thousands of packages to defense contractors in the U.S. The memo offered a special service – early warning notification of foreign observation flights, cost-free. You may have received one too. More importantly, if you took the time to fill in the requested information and subscribe to the service, you could have already received early warning notification of U.S.-foreign joint observation training flights occurring over the United States.

This is the sixth in a series about the Open Skies Treaty prepared by the On-Site Inspection Agency (OSIA) to increase *Readiness Through Awareness* within the defense contractor community. It is intended to increase awareness among site and facility managers, facility security officers and senior company officials of arms control activities that can affect defense industry sites in the United States. The purpose of this article is to introduce procedures established by the Defense Department to notify vulnerable sites about observation flights conducted under the Treaty on Open Skies. Forewarned defense and industry sites can then take appropriate measures to protect sensitive and proprietary information.

The United States took another step aimed at increasing confidence and security in the world when it ratified the Treaty on Open Skies in December 1993. Originally proposed by President Eisenhower in 1955, the Treaty was reintroduced by President Bush in 1989 and signed in Helsinki on March 24, 1992. The Treaty promotes transparency in military arms and acts as an important confidence building measure by permitting its members to overfly each other's territory using aircraft equipped with cameras, synthetic aperture radar and infrared sensors.

As a Treaty member, the United States may receive as many as 42 Open Skies overflights per year. Because all areas are subject to overflight, during daylight or darkness, some operations at defense industrial sites could be affected. However, because Treaty members requesting to overfly U.S. territory must provide 72 hours notice, the Defense Department can provide early warning notification to vulnerable sites. Furthermore, the duration of a site's vulnerability is limited because each overflight must be completed within 96 hours after the observation team arrives in the U.S.

As soon as Mike hung up, Larry reached for a growing folder on the corner of his desk labeled Treaty Security Information. Luckily, he had just received something about Open Skies – a DTIRP security information bulletin. He grabbed the bulletin and hurried over to Mike's office, re-reading it as he walked. Larry handed the bulletin to Mike saying, "I received this just yesterday, it's from the Defense Department's On-Site Inspection Agency in Washington. As Mike read the bulletin, Larry noticed the package on Mike's desk was also from OSIA, "Just as I hoped" he said to himself. Mike finished reading the bulletin then exclaimed, "Airplanes fly over everyday, and there probably are satellites too, why should I be concerned if a few more planes fly over?" Larry began to explain the sensors that are permitted by the Treaty and how the collected data must be shared with any signatory willing to pay the cost of reproduction. Larry was concerned about potential impact to the DX-5 pro-

gram's research, development, test and evaluation activities at Defense Tech ...

Three types of devices – optical cameras, synthetic aperture radar, and infrared sensors – are permitted on board Open Skies aircraft to record objects on the ground during the observation flight. However, in recognition of each signatory's need to protect highly sensitive information, the Treaty places limitations on the capabilities of the sensors. This is accomplished by limiting the "ground resolution" of the image that the sensor can collect. Simply defined, ground resolution is the minimum distance between two objects at which an observer can tell they are separate objects.

For example, the maximum ground resolution of images recorded by optical panoramic, framing and video cameras may not exceed 30 centimeters. Moreover, this resolution cannot be obtained at a distance greater than 50km or roughly 31 miles. So, the Open Skies aircraft must come within 50km of your site to obtain the permitted resolution and therefore the best possible images. Images can be incidentally collected beyond the 50km limit, for example if the aircraft tipped due to air turbulence, but the images will have degraded resolution and therefore be of less use to the observing party. A simplified example of this kind of image occurs when an ordinary camera is focused on a subject three feet away; an image of the background scenery is also captured in the photograph, but it appears out of focus and somewhat blurred. In this example, the optimum camera range is three feet.

While panoramic and framing cameras are likely to be the most common sensors used during the first three years of the Treaty, synthetic aperture radar (SAR) may also be used. The resolution of SAR for Open Skies overflights is restricted to 3 meters. The third type of sensor is an infrared line-scanner. But, these are not allowed during the first three years of the Treaty except by mutual agreement of both Treaty members. When it is used, the ground resolution is restricted to 50cm.

Despite these restrictions, imagery collected during Open Skies overflights will provide a significant amount of information that cannot be acquired by commercial satellites. Open Skies sensor limits were established to allow observation teams to distinguish a tank from a truck, and to identify large military equipment and aircraft during an overflight. Consequently, the sensors can also detect a range of outdoor industrial equipment and vehicles, and reveal facility layouts and security arrangements. Moreover, unlike satellites, some Open Skies sensors can be mounted obliquely to image at an angle sideways from the flight path, thereby recording some objects that are covered or just inside large open doorways. Likewise, with simultaneous use of multiple cameras, the combination of vertical and oblique photographs can be overlapped to provide three-dimensional images which may also reveal the height and side characteristics of objects.

In addition to the optical sensor's capabilities, SAR and infrared sensors present added challenges to some facilities because both sensors can image through certain materials and thin coverings, such as wood, canvas, etc., and both work equally well night or day. Finally, synthetic aperture radar even performs well during inclement weather.

"Well Larry, you make it sound like something from a Star Trek television script," Mike said, "but, what does it really mean to us here at Defense Tech? You know I just got the Test and Evaluation Master Plan approved for the DX-5, and the prototype will be ready to begin outdoor testing in less than ten weeks." "I'm no expert on these sensors Mike," Larry said, "but I have some other information I picked up last month at our annual security convention. Give me some time to pull it all together and get you a better answer." Fortunately for Larry, representatives from OSIA and the Defense Investigative Service were also at the convention to provide information about the potential impact of arms control activities. Larry had picked up several items and put them in his new Treaty Security Information folder. "Here it is, Open Skies Treaty–The Impact," Larry said aloud as he opened the pamphlet from OSIA.

As you would suspect, Open Skies overflights will primarily affect activities that occur outdoors, such as research, development, testing and evaluation or modification programs. But plant and facility layouts will be readily observable,

including such items as new construction, power sources, ventilation systems, physical security arrangements, external storage areas, shipping containers, parking lot and road capacity and use, cooling ponds, thermal pollution of waterways and pollution of vegetation. Thermal images from infrared sensors may also reveal information on production activities and the level and scope of heat generating activities *inside* of a facility.

All of these items could be useful in creating an intelligence mosaic of a facility and its operations. This type of information can also be valuable in filling in the missing pieces of an intelligence picture that has been created from other sources. This is particularly important for defense industry because of increased emphasis on economic intelligence collection by many countries.

Finally, the Open Skies Treaty will provide many nations with their first opportunity to conduct aerial observations over the United States. Consequently, a considerable amount of information could be collected which may not have been previously available to them. Additionally, other Treaty members who previously relied upon commercial satellite imagery purchased abroad, can purchase copies of all imagery from Open Skies overflights.

The next day Mike was more concerned about the DX-5 project's vulnerability to Open Skies overflights. He saw Larry in the hall and asked, "Could you take a look at the Test & Evaluation Master Plan and find out if the prototype DX-5 test schedule will be affected by an overflight? Let me know what you come up with as soon as possible." Larry got back to his office and thought for a moment. It must have seemed like a daunting task for Mike to give, but Larry knew just who to call for help on arms control treaty implementation issues...

Established by the Defense Department, the Defense Treaty Inspection Readiness Program (DTIRP) provides assistance to the Defense Department, and the defense contractor community in particular, in protecting national security, proprietary and other sensitive information during arms control activities like Open Skies overflights. The Defense Department's Executive Agent for DTIRP, the On-Site Inspection Agency, created a system to notify any site or facility that may be imaged during an observation flight. OSIA can help managers at facilities like Defense Tech to minimize the security impact of Open Skies Treaty overflights. Representatives from the Defense Investigative Service (DIS) can also provide valuable assistance.

Larry opened the Open Skies Treaty Data Call package Mike had received the day before. It was exactly what he hoped for – the Passive Overflight Module Data Preparation Instructions he requested from OSIA only last week. Larry knew that by filling in and submitting the data call package, Defense Tech could subscribe to a cost-free service and have their site entered into a notification database within the Passive Overflight Module (POM).

The POM allows the On-Site Inspection Agency's Security Office personnel to analyze the flight path of a proposed Open Skies overflight and determine potential sensor coverage and resolution along the route. This is then provided to OSIA's 24-hour Operations Center to notify those facilities which might be affected by an impending overflight. This is done through the Telephone Notification System or TNS – an automated system which sends POM-generated notifications to all sites which may be imaged along the flight path of a proposed mission. The initial warning of an intent to fly is provided to facilities at least 96 hours before the observation flight begins, with regular updates on site vulnerability including the time of possible sensor coverage. Messages are transmitted over standard phone lines, but can include a variety of formats including facsimile, modem, pager, answering machine or voice mail. TNS messages can also be transmitted over the Automated Digital Network (AUTODIN) message system. Of course, you cannot receive the notifications if you haven't subscribed to the service.

One week later... "Well Larry, what have you come up with?" Mike asked. "Mike, what would you say if I could give you advance warning of every Open Skies overflight that could image our site?!" Larry said enthusiastically. Before Mike could answer, Larry continued, "I've added all Defense Tech facilities to a

database and notification system developed by the Defense Department. From now on we will receive...."

The Treaty on Open Skies will allow many nations to obtain imagery taken over any part of the United States and its territories. But, with advance warning through OSIA's Passive Overflight Module and Telephone Notification System, concerned defense sites and industrial facilities can take appropriate measures to preclude the loss of sensitive or proprietary information. For more information about U.S. Government assistance that is available, call the On-Site Inspection Agency's Industry Outreach Program Manager at 1-800-419-2899, or contact your local DIS representative.

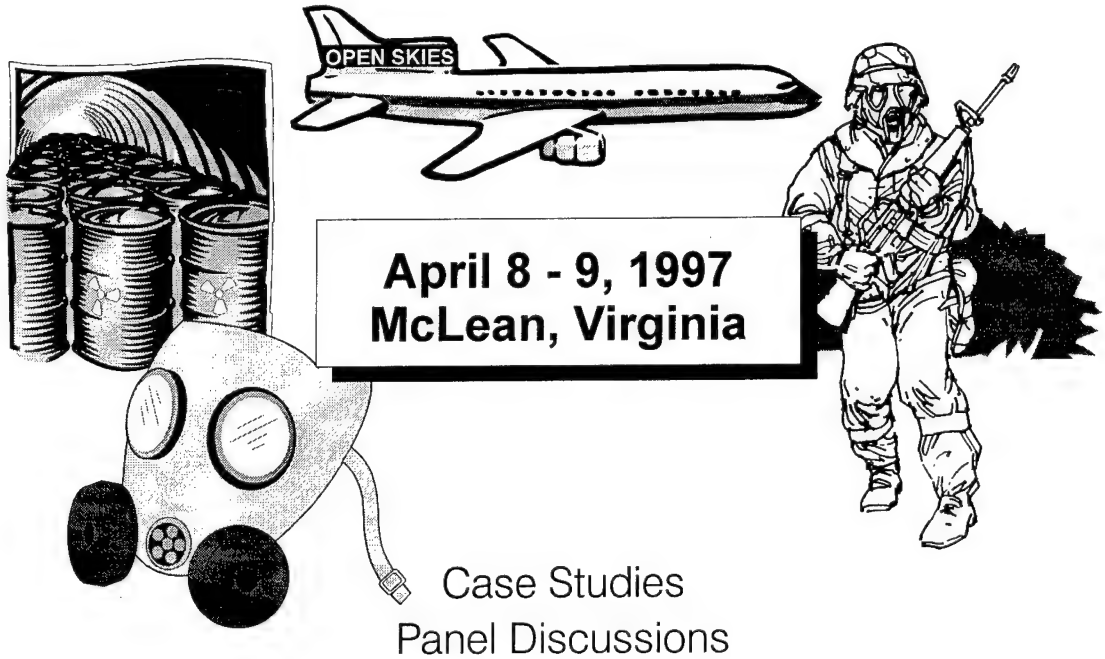
Defense Treaty Inspection Readiness Program

NATIONAL SEMINAR

Focus of this year's seminar
is the

Chemical Weapons Convention

Entry Into Force 29, April 97



April 8 - 9, 1997
McLean, Virginia

Case Studies
Panel Discussions
Facility Negotiations
Technical Equipment Issues
Arms Control Security Overview
Chemical Weapons Convention Overview
CWC Challenge Inspection/Managed Access

To register or for more information call: 1-800-419-2899
or visit the DTRIP homepage @ www.OSIA.mil

Now available from the On-Site Inspection Agency:

The United States is partner to a host of international treaties designed to develop trust and cooperation among nations while reducing or eliminating weapons of mass destruction. To be successful, treaty partners must grant openness. In the arms control environment this means permitting highly intrusive verification activities. The DoD has developed the Defense Treaty Inspection Readiness program (DTIRP) to manage this inspection process without risking loss of sensitive information.

The catalog lists a variety of materials you can order to prepare your company or organization for inspections:

- **Security Information Bulletins** for facility security officers and managers provide potential implications of inspection and overflight activities, and government help available for a facility. Issued five times a year, or more often when required.
- **Information pamphlets** aim to help facility personnel quickly orient themselves with arms control agreements and their inspection provisions. Four published a year.
- **Video presentations** on the potential impact of arms control agreements on U.S. facilities, treaty-specific inspection implementation concepts, methodology/resources/capabilities of DTIRP, types of government assistance, and more. Videos are 10- to 40-minutes long.
- **Articles** on arms control security information written in an interesting and easily read format. Four articles are planned each year.
- **Circulars, mailers, and brochures** to hand out at conventions, seminars, and meetings. Written as concise introductions to particular subjects.

For copies call 1-800-419-2899 or write:
Attn: Security Officer
On-Site Inspection Agency
201 W. Service Rd., Dulles IAP
P.O. Box 17498
Washington, DC 20041-0498

http://www.osia.mil

What's new
in DoDSI's independent study courses

They're NISPOM-keyed. Updates to the following are now available for enrollment:

- Essentials of Industrial Security Management (EISM), DS 2123,
- Protecting SECRET and CONFIDENTIAL Documents (PSCD), DS 2124, and
- Basic Industrial Security for User Agency Personnel (DS 2121)

They cost. Beginning August 1, 1996, a fee of $27.50 will be charged for all DoDSI courses administered through the Army Institute for Professional Development (AIPD) at Newport News, Virginia. This basic service charge enables us to defray the costs of printing and shipping the course materials and of providing enrollment, student services, test grading, record-keeping and other services through AIPD.

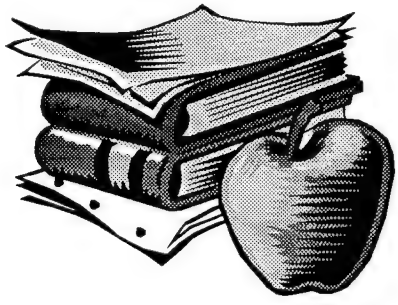
How to pay. Payment must accompany your application and is non-refundable. Payment by personal check or by personal or organizational credit card is not acceptable. Acceptable forms of payment are:

NEW!
- Company check made payable to "Deputy Director for Finance."
- Money order made payable to "Deputy Director for Finance."
- Certified check made payable to "Deputy Director for Finance."
- DD Form 1556, Request, Authorization, Agreement, Certification of Training and Reimbursement. In block 19a enter "Army Inst. for Professional Dev." In block 19b enter

  U.S. Army Training Support Center
  Newport News, VA 23628-9989
- SF 1080, Voucher for Transfer of Funds. Funds should be transferred to the following address:

  USATSC
  ATTN: ATIC-RMB
  Bldg 1747
  Fort Eustis, VA 23604-5166

For more information. A complete description of courses and enrollment procedures is in the *DoDSI's Info Guide FY 1997*. If you don't have access to one, please fax your request and complete mailing address to: (804) 279-6406 or DSN 695-6406, Attn: Info Guide. The *Info Guide* and schedule is also on our Web page: http://www.dtic.mil/dodsi.



The San Diego Industrial Security Council

is presenting

The 7th Annual
Security Awareness Seminar

May 21st and 22nd, 1997

at the beautiful
Mission Valley Town & Country Hotel
San Diego, California

There will be workshops on security education, NISPOM basics, Internet security, protection of proprietary information, and other security related topics. This confluence of relevant subjects will give you the greatest "bang for the buck" for information and strategies that can be brought back to your company to use and share with your management and employees.

The fee for the two-day seminar is only $97.00. This includes pastries, beverages and validated parking. Lunch on the second day is a pool side theme – BEACH PARTY BUFFET – and all the attendees are encouraged to come dressed in their finest Hawaiian dress or shirt.

To register, send in your fee and the completed form on the back of this page. Have a question? Contact seminar co-chairs **Patti Adams**, SAIC, (619)546-6595) [patti_adams@cpqm.saic.com] or **Craig Packard**, DIS (619) 674-4211 [packardc@dislink.jcte.jcs.mil].

REGISTRATION FORM

INDUSTRIAL SECURITY TRAINING SEMINAR
TOWN & COUNTRY HOTEL
SAN DIEGO, CALIFORNIA
MAY 21 & 22, 1997

(Please use separate sheet for each attendee)

[Please PRINT or TYPE all information]

NAME: _____ _____
(Last) (First)

COMPANY / AFFILIATION: _____

MAILING ADDRESS: _____

_____

_____

TELEPHONE: (___) _____ **FAX:** (___) _____

E-MAIL ADDRESS: _____

Please enclose your check for $97.00, to cover the Seminar Fee, for each attendee. Make checks payable to: SAN DIEGO ISAC and mail to:

Jeannie Schoewe
10730-58 Aderman Avenue
San Diego, CA 92126-2569

Statistical Information Request

- Current security responsibilities: (√)

_____FSO _____Assistant FSO _____Security Staff Member _____Document Custodian

_____COMSEC Custodian _____CSSO _____Other: _____

- How long have you held security responsibilities ?_____
- What specific question(s) would you like addressed during the seminar ?

_____

(please use back for additional questions)

SPECIAL NOTE: The San Diego ISAC is a non-profit organization with a California tax ID of 93-1046554. As such, your educational fees for attendance at this seminar are tax deductible by your organization.

Downlink DoDSI

A Video Teletraining Course

You can now take DoD Security Institute's "Protecting Classified National Security Information" course via video teletraining. Video teletraining uses a satellite and television equipment to "beam" the instructor live into your local classroom on a television screen. Microphones and communication buttons on each student desk allow you to participate in discussion or ask questions, and get immediate answers from the instructor.

We call it "Downlink DoDSI."

About the course

"Protecting Classified National Security Information" is a three-day course designed to help people gain the skills and information needed to work successfully with classified information. It is ideally suited for unit/additional duty security managers and helpful for anyone who routinely works with classified information. It includes

- basic classification management
- marking, safeguarding
- storing, transmitting
- destruction, and
- security in today's technical office.

The course was specifically developed for video teletraining. To optimize the use of costly satellite time, additional learning takes place during facilitator-led activities. Twelve hours of instruction and discussion are broadcast via television and an additional six hours of instruction is conducted by a security subject matter expert from your activity.

The course lasts three days, each day consisting of four hours of video teletraining and two hours of subject matter expert (SME) facilitator-led activity. Facilitator-led activities include practical exercises, quizzes, directed discussions, etc. These activities enhance, reinforce, and provide practical application for material introduced by the broadcast. Each site must provide an SME security facilitator to assist the DoDSI faculty in conducting the course. The facilitator performs administrative functions, handles technical problems, leads off-line exercises, and administers an end-of-course exam.

Students successfully completing the course receive a certificate of training.

About the technology

Downlink DoDSI is currently broadcasting over the Satellite Education Network, from its studios at the Army Logistics Management College, Fort Lee, Virginia. The 3.3 compressed, digital signal is uplinked to the Telstar 401 satellite and downlinked to a receiving site that is bridged via telephone lines back to the studios in Virginia, permitting real-time audio communications. This system allows for interaction between the faculty and the training locations receiving the broadcast.

- 3 days of class
- 12 hours video teletraining
- 6 hours with on-site facilitator
- real-time audio communications
- faculty and student interaction

Class dates

1997
April 22-24
July 22-24
September 30-October 2

For additional details or information on how to host this course, call Ray Dion, DSN 695-5140 or Commercial (804) 279-5140, or Cheryl Cross ext. 4390.

NATIONAL OPSEC CONFERENCE AND EXHIBITION

MCLEAN HILTON HOTEL, TYSONS CORNER, VIRGINIA

MAY 4-8, 1997

HOSTED BY OPSEC PROFESSIONAL SOCIETY AND THE INTERAGENCY OPSEC SUPPORT STAFF

The 1997 National OPSEC Conference will focus on the application of OPSEC throughout government and industry. Beginners and experts will find interesting and challenging sessions and workshops to attend!

Monday Classified Sessions

TOPICS:

- OPSEC Lessons Learned
- Information Warfare
- Terrorism on the INTERNET
- Current HUMINT Threat

Tuesday, Wednesday & Thursday Unclassified Sessions/Workshops

On Tuesday, a one-day Introduction to OPSEC Course will be offered, sponsored by the General Services Administration and taught by experts in the field. This course is designed to provide an overview of OPSEC concepts and practices, and a familiarity with OPSEC terminology. There is no additional fee for the course.

OTHER TECHNICAL TOPICS:

- Risk Assessment
- Information Systems Vulnerabilities & Risks
- OPSEC Applications in the Commercial Sector
- Commercial Imagery
- Information Terrorism
- SIGINT Threat
- Law Enforcement
- Threats to University-based Research
- Perception Management
- INTERNET Threats & Vulnerabilities
- Information Warfare
- Counterintelligence & Security

WORKSHOPS

- Law Enforcement
- OPSEC Program Management
- Risk Assessment
- Creative OPSEC Awareness
- Treaties
- OPSEC Applications in the Commercial Sector

ACCOMMODATIONS

The McLean Hilton at Tysons Corner will be the official headquarters for the conference and exhibition. Rooms have been reserved at the prevailing government rate for government and industry. To make reservations, please call 1-800-HILTONS or (703) 761-5111. Please mention the OPSEC Professionals Society/IOSS when making your reservation. Reservations must be made by April 4, 1997.

McLean Hilton at Tysons Corner
7920 Jones Branch Drive
McLean, VA 22102-3308
(703) 847-5000

Dulles and Washington National Airports are both conveniently located near the McLean Hilton. The McLean Hilton offers complimentary parking and provides complimentary van shuttle service between West Falls Church Metro and the hotel.

CANCELLATION POLICY

Refunds will ONLY be made for written cancellations received by April 18, 1997. After that date only personnel substitutions may be made. Telephone cancellations will not be accepted.

NATIONAL OPSEC AWARDS LUNCHEON

The 1997 Individual, organizational, and Audio-Visual OPSEC Achievement Awards will be presented at the National OPSEC Awards Luncheon on Wednesday, May 7 (included in your registration fee).
The National OPSEC Awards Program was instituted to recognized significant contributions to the OPSEC discipline.

OPS ANNUAL MEMBERSHIP MEETING / DINNER

The OPS Annual Dinner will be held on Tuesday evening, May 6. After dinner, OPS will hold its annual business meeting. Additional information for this event will be mailed under separate cover or you may call OPS at (301) 840-6770.

OCP LUNCHEON

For the first time a special luncheon will be held for all OPSEC Certified Professionals. This invitation is extended to all current OCPs. The luncheon will be held on Thursday, May 8 at 11:30 a.m. The cost is $10. Please leave time in your schedule to attend.

National OPSEC Conference and Exhibition

May 4-8, 1997 McLean Hilton Hotel Tysons Corner, Virginia

REGISTRATION FORM

Send to: OPSEC Professionals Society, 9200 Centerway Road, Gaithersburg, MD 20879
or FAX: (301) 840-8502

Please complete one form for each person attending. Information will be used to produce the conference networking list, which will be provided as part of the conference package.

If you wish to have your information withheld from the list, please check here. ☐

Name: _____ Organization/Company: _____

Address: _____

Commercial Phone (no DSN): _____ FAX: _____ E-mail: _____

How would you like your name to appear on your badge? _____

How would you like your organization/company name to appear on your badge?

as above ☐ none ☐ other ☐ _____

Please register me for the Introduction to OPSEC Course, Tuesday, May 6. ☐

Please register me for the OCP Luncheon on Thursday, May 8 for an additional charge of $10. ☐

Are you an OPSEC Certified Professional? (OCP) yes ☐ no ☐

Are you attending the National OPSEC Conference & Exhibition for the first time? yes ☐ no ☐

Admission to the Classified Sessions will require you to first sign-in at the Conference Registration Desk at the Hilton.

Fees include Conference, Proceedings, Breaks, Awards Luncheon, and Reception.

PLEASE CIRCLE APPROPRIATE FEE		Classified Only	Conference Only	Both
Before March 14	OPS Member	$60	$415	$465
	Nonmember	$60	$450	$500
After March 14	OPS Member	$60	$465	$515
	Nonmember	$60	$500	$550

If you pay as a nonmember, and you have never been a member of OPS, you receive a complimentary membership for 1997.

Amount Enclosed [ ] DD 1556 or SF 182 Enclosed ☐

Payment may be made by check, money order, government training form, VISA, MasterCard or American Express. Checks and money orders should be made payable to OPSEC Professionals Society. You may FAX a copy of the training form with your registration form, but please be prepared to turn in the original when you arrive on site. Those using training forms should ensure that payment is made promptly at conclusion of the conference.

Credit Card Payment: ☐ VISA ☐ MasterCard ☐ American Express

Card Number: _____ Expiration Date: _____

Name on Card: _____ Signature: _____

National OPSEC Conference and Exhibition

May 4-8, 1997 **McLean Hilton Hotel** **Tysons Corner, Virginia** **SECRET U.S. Only**

SECURITY FORM

THERE WILL BE NO PROVISION FOR SECURITY CLEARANCE CERTIFICATION AT THE CONFERENCE. CLEARANCES NEEDED TO ATTEND CLASSIFIED TECHNICAL SESSIONS ONLY.

This security form is for U.S. Citizens only.

NAME:_____

TITLE OR POSITION:_____

AFFILIATION/COMPANY:_____

BUSINESS ADDRESS:_____

PHONE:_____ FAX:_____

(Please provide commercial numbers)

DATE AND PLACE OF BIRTH:_____

SOCIAL SECURITY NUMBER:_____

SIGNATURE:_____

TO BE COMPLETED BY SECURITY OFFICER: I certify the above person has been granted a security clearance of SECRET or higher.

ISSUING AGENCY & DATE ISSUED:_____

LEVEL OF CLEARANCE:_____

PHONE:_____

SECURITY OFFICER NAME:_____

SECURITY OFFICER SIGNATURE:_____

DATE:_____

FORMS MUST BE RECEIVED BY APRIL 18:

Interagency OPSEC Support Staff
6411 Ivy Lane
Suite 400
Greenbelt, MD 20770-1405
Secure Fax: (301) 982-0319

ATTN: Security Office

Questions?? (301) 982-0323

Attention Security Educators, here's your chance to sign up for the:

Train-the-Trainer/Security Briefers Course!

Train-the-Trainer/Security Briefers Course will be offered at the DoD Security Institute in Richmond, Virginia, on these dates

Train-the-Trainer	Security Briefers Course
March 17-21, 1997	March 19-21, 1997
June 23-27, 1997	June 25-27, 1997
September 8-12, 1997	September 10-12, 1997

If interested in attending any of the above classes, please mail or fax us the Registration Form on the next page. The fax is (804) 279-6406, DSN 695-6406.

Also,

The Security Awareness and Education Subcommittee is sponsoring a **Security Briefers Course** to be held at the Department of Commerce, Washington, DC.
Dates: 26-28 March 1997
If you'd like to attend, fax us the Registration Form on the next page.
The fax number is (804) 279-6155, DSN 695-6155. Points of contact are:
Gussie Scardina (804) 279-5308 and Linda Braxton (804) 279-6076. DSN is 695-xxxx.

If you'd like to *host* this course, call Linda Braxton at (804) 279-6076, DSN 695-6076.

About the course:

The **Security Briefers Course** prepares security professionals to plan and deliver effective security briefings. Activities include preparing a briefing plan; presenting a briefing in a clear and interesting manner; designing and using briefing aids; and evaluating the effectiveness of an oral briefing.

Train-the-Trainer prepares security specialists to *teach* the Security Briefers Course (SBC) 5220.13. It begins as a two-day instructor preparation workshop before the first day of the SBC. The next three days are spent *teaching* the SBC under the supervision of DoDSI staff. Graduates return to their organization with Security Briefers Course instructor guide, workbook, and student handout packet. Activities include using the SBC materials, teaching the lessons in the SBC, assisting others to prepare briefing plans, and conducting practice briefing sessions.

Security Awareness Bulletin

Subscription Service

As we announced in our last issue, beginning with the first quarter of 1997, the *Security Awareness Bulletin* can no longer be distributed free of charge to Defense contractors and to non-Defense agencies.

But the good news is that anyone can get the *Bulletin* one of two ways:

1. By accessing our DoDSI web page (http://www.dtic.mil/dodsi). We will send you an automatic e-mail notice via the Internet when a new issue goes on-line. Just enter your e-mail address on the registration form for this service in the *Security Awareness Bulletin* section of our web page.

2. By signing up for a low-cost subscription service that we have arranged through the U.S. Superintendent of Documents.

Here's how the Bulletin Subscription Service works: Send in a copy of the form below with a check for the appropriate amount and you will receive the *Bulletin* four times a year.

United States Government
INFORMATION

Order Processing Code
*5769

Credit card orders are welcome!

Fax your orders (202) 512-2250
Phone your orders (202) 512-1800

Security Awareness Bulletin at $9.00 ($11.25 foreign) per year
The total cost of my order is $ _____.

☐ YES, please send _____ subscription(s) to:

_____
Name or title (Please type or print)

_____
Company name Room, floor, suite

_____
Street address

_____
City State Zip +4

_____
Daytime phone including area code

_____
Purchase order number (optional)

For privacy protection, check the box below:
☐ Do not make my name available to other mailers

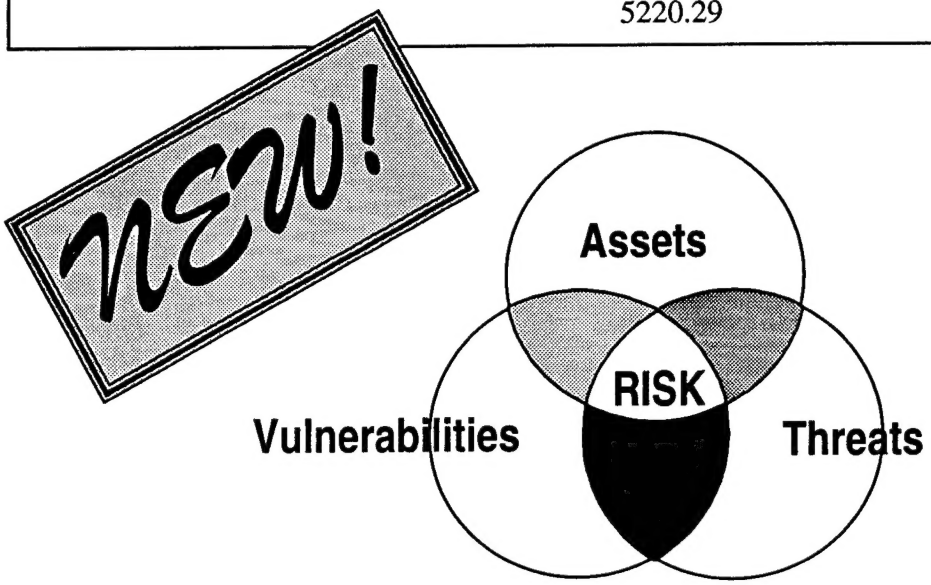
Check method of payment:
☐ Check payable to: Superintendent of Documents
☐ GPO Deposit Account ☐☐☐☐☐☐☐–☐
☐ Visa ☐ MasterCard
☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐
(expiration date)
☐☐☐☐

_____
Authorizing signature

Mail to:
Superintendent of Documents, PO Box 371954, Pittsburgh PA 15250-7954
Important: Please include this completed order form with your remittance. *Thank you for your order!*

Risk Management for DoD Security Programs

5220.29



Countermeasures

Obtain the background, skills, and abilities to apply risk management principles and methodology to the implementation of DoD security programs.

The course covers fundamentals of risk management, asset assessment, threat assessment, vulnerability assessment, risk analysis, and the selection of cost effective countermeasures to apply as a result of the process.

Who Should Attend:

Risk managers
Security personnel
Program managers
Others, as appropriate

Government and Government Contractors Only

Call Carl Roper at DSN 695-5593, COMM [804] 279-5593
or Mark Reardon DSN 695-5170 for information

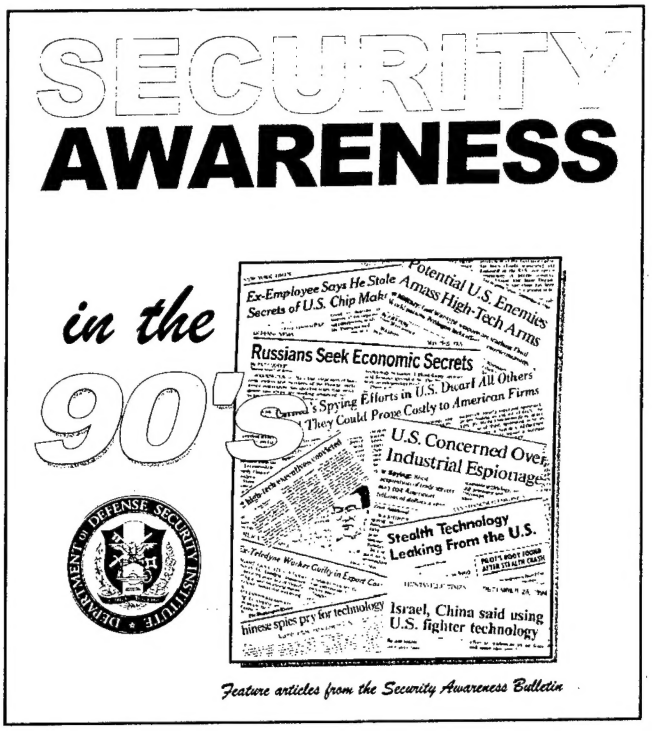
Course scheduling for FY98 will be available in mid-summer

Security Awareness in the 1990s

feature articles from the
Security Awareness Bulletin 1990-1996

Subject areas:

- the foreign intelligence threat
- espionage case studies
- industrial security
- information systems security
- security policy and programs
- the threat to U.S. industry



This is the second compilation of past *Bulletin* articles issued by the DoD Security Institute. The first volume, Security Awareness in the 1980s, was published in 1990 and was an immediate success. The new edition picks up where the former left off. It will be particularly useful to younger security professionals who didn't see these articles when they first appeared.

*U.S. Government Printing Office: 1997 - 527-109/60002

Superintendent of Documents **Publication** Order Form

Order Processing Code
*8012

___ copies of **Security Awareness in the 1990s,** S/N 008-047-00409-5 at $22.00 each ($27.50 foreign).

The total cost of my order is $ _____. Price includes regular shipping and handling and is subject to change.

Name or title (Please type or print)

Company name Room, floor, suite

Street address

City State Zip +4

Daytime phone including area code

Purchase order number (optional)

Check method of payment:

☐ Check payable to: Superintendent of Documents

☐ GPO Deposit Account ☐☐☐☐☐☐☐—☐

☐ Visa ☐ MasterCard

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

(expiration date)

☐☐☐☐

Thank you for your order!

Authorizing signature

Mail to: Superintendent of Documents, PO Box 371954, Pittsburgh PA 15250-7954

Security Awareness Publications Available from the Institute

Publications are free. Just check the titles you want and send this form to us with your **address label**

Our address is:

DoD Security Institute
Attn: SEAT
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, VA 23297-5091
(804) 279-4223 or DSN 695-4223

- ❑ **Recent Espionage Cases: Summaries and Sources.** May 1996. Eighty-eight cases, 1975 through 1995. "Thumb-nail" summaries and open-source citations.
- ❑ **Announcement of Products and Resources.** October 1996. A catalog of security education videos, publications, posters, and more you can order.
- ❑ **DELIVER!** Easy-to-follow pamphlet on how to transmit and transport your classified materials. Written specifically for the Department of Defense employee. September 1992.
- ❑ **Terminator VIII.** Requirements for destruction of classified materials. Written specifically for the Department of Defense employee. September 1992.
- ❑ **STU-III Handbook for Industry.** To assist FSOs of cleared defense contractors who require the STU-III, Type 1 unit. Covers step-by-step what you need to know and do to make the STU-III a valuable addition to your facility's operations.
- ❑ **Survival Handbook.** The basic security procedures necessary for keeping you out of trouble. Written specifically for the Department of Defense employee. April 1995.
- ❑ **Layman's Guide to Security.** The basic security procedures that you should be aware of when handling classified materials in your work environment. May 1995.
- ❑ **Acronyms and Abbreviations.** Twelve pages of security-related acronyms and abbreviations and basic security forms. October 1995.
- ❑ **Take A Security Break.** Questions and answers on security and other topics.
- ❑ **Take Another Security Break.** More questions and answers.
- ❑ **Lock Up!** A pamphlet on the structural standards and other security requirements for the storage of conventional arms, ammunition, and explosives. August 1995.

Security Awareness Bulletin. A quarterly publication of current security countermeasures and counterintelligence developments, training aids, and education articles. Back issues available from the Institute:

- ❑ The Case of Randy Miles Jeffries **(2-90)**
- ❑ Beyond Compliance - Achieving Excellence in Industrial Security **(3-90)**
- ❑ Foreign Intelligence Threat for the 1990s **(4-90)**
- ❑ Regional Cooperation for Security Education **(1-91)**
- ❑ AIS Security **(2-91)**
- ❑ Economic Espionage **(1-92)**
- ❑ OPSEC **(3-92)**
- ❑ What is the Threat and the New Strategy? **(4-92)**
- ❑ Acquisition Systems Protection **(1-93)**
- ❑ Treaty Inspections and Security **(2-93)**
- ❑ Research on Espionage **(1-94)**
- ❑ Acquisition Systems Protection Program **(3-94)**
- ❑ Aldrich H. Ames Espionage Case **(4-94)**
- ❑ Revised Self-Inspection Handbook/Summary of NISPOM Changes **(1-95)**
- ❑ The Threat to U.S. Technology **(2-95)**
- ❑ Entering a New Era in Security **(1-96)**
- ❑ Technical Security **(2-96)**
- ❑ Combating Terrorism **(3-96)**
- ❑ Profile of a Spy **(1-97)**